Tutorial 8: Number theory I

Department of Computer Science and Engineering
Hong Kong University of Science and Technology

Question 1

(a) Let m and n be two positive integers such that m divides n, i.e., $n = sm$ for some other integer s. Show that, for any integer x,

$$(x \bmod n) \bmod m = x \bmod m.$$

(b) For each number in Z_8, state if it has a multiplicative inverse mod 8, and if it has, state its inverse. There is no need to explain your answer.

Question 1

Solution:

(a) Let $x \bmod n = r_1$. Then $x = q_1 n + r_1$ for some integer q_1. Further let $r_1 \bmod m = r_2$. Then $r_1 = q_2 m + r_2$ for some integer q_2. Hence,

$$x = q_1 n + q_2 m + r_2 = q_1 sm + q_2 m + r_2 = (q_1 s + q_2)m + r_2$$

where $0 \leq r_2 < m$. Consequently,

$$x \bmod m = r_2 = (x \bmod n) \bmod m.$$

(b) 0 has no inverse; 1's inverse is 1; 2 has no inverse; 3's inverse is 3; 4 has no inverse; 5's inverse is 5; 6 has no inverse; 7's inverse is 7.

Question 2

Let a, m and n be three positive integers that are larger than 1. Is each of the following statements true or false? If it is true, give a proof. If it is false, give a counterexample.

(a) $(a \bmod mn) \bmod n = a \bmod n$.

(b) $(a \bmod mn) \bmod n = a \bmod m$.

(c) If $a \bmod n = 1$, then $gcd(a, n) = 1$.

(d) If $gcd(a, n) = 1$, then $a \bmod n = 1$.

Question 2

Solution:

(a) This is true. According to Euclid's Division Theorem, there exist q_1 and r_1 such that

$$a = q_1 mn + r_1, \quad 0 \le r_1 < mn,$$

where $r_1 = (a \bmod mn)$. Similarly, there exist q_2 and r_2 such that

$$r_1 = q_2 n + r_2, \quad 0 \le r_2 < n,$$

where $r_2 = r_1 \bmod n = (a \bmod mn) \bmod n$. Combining the two equations, we get

$$a = (q_1 m + q_2) n + r_2, \quad 0 \le r_2 < n.$$

Hence, $a \bmod n = r_2$. Consequently,

$$(a \bmod mn) \bmod n = r_2 = a \bmod n.$$

(b) This is false. Let $a = 8, m = 2$ and $n = 3$. We have

$$\begin{aligned}(a \bmod mn) \bmod n &= (8 \bmod 6) \bmod 3 = 2,\\ a \bmod m &= 8 \bmod 2 = 0.\end{aligned}$$

(c) This is true. $a \bmod n = 1$ implies that there exist q such that $a = qn + 1$, or $a - qn = 1$. The latter equation implies that any common divisor of a and n must divide 1, hence must be 1. Therefore, $gcd(a, n) = 1$.

(d) This is false. For example, $gcd(5, 3) = 1$, but $5 \bmod 3 = 2$.

Question 3

Let a, b, m and n be positive integers. Suppose

$$a \bmod m = b \bmod m, \quad n|m.$$

Prove the following equations:

(a) $a \bmod n = b \bmod n$.

(b) $a^2 \bmod m = b^2 \bmod m$.

Solution:

(a) Since $n|m$, it holds that $m = tn$ for some integer t. Moreover, $a \bmod m = b \bmod m$ implies $(a - b) \bmod m = 0$, which in turn implies there exists integer q such that

$$\begin{aligned} & (a-b) = qm \\ \rightarrow \quad & (a-b) = qtn. \end{aligned}$$

So n divides $(a - b)$. This implies $(a - b) \bmod n = 0$, which in turn implies $a \bmod n = b \bmod n$.

(b) As shown earlier, $(a - b) = qm$ for some q. Multiplying both sides with $(a + b)$, we get

$$a^2 - b^2 = (a+b)(a-b) = (a+b)qm.$$

So m divides $a^2 - b^2$. This implies that $a^2 - b^2 \bmod m = 0$, which in turn implies that $a^2 \bmod m = b^2 \bmod m$.

Question 4

Does there exist an x in Z_{154} that solves

$$21 \cdot_{154} x = 5?$$

if yes, give the value of x (it is not necessary to show your work).
If no, prove that such an x does not exist.

Question 4

Solution:
No. First note that $21 = 3 \cdot 7$ and $154 = 22 \cdot 7$.
If there was such an x then $21x = 154q + 5$ for some q.
Then $5 = 21x - 154q = 7(3x - 22q)$
Since 7 does not divide 5, this is impossible.

Note that to solve this problem it would not have been enough to say that "$gcd(21, 154) = 7 \neq 1$ so 21 does not have an inverse in Z_{154}."

Some problems in the form

$$21 \cdot_{154} x = b$$

actually do have solutions $x \in Z_{154}$. For example

$$21 \cdot_{154} x = 42$$

has the solution $x = 2$.